

**WHAT IS CLAIMED IS:**

1. A method for updating an inherent key-encrypted program in a system including an LSI device and an external memory, the inherent key-encrypted program being generated by encryption with an inherent key unique to the LSI device and being stored in the external memory, the method comprising:
  - a first step of receiving by the system a common key-encrypted program generated by encryption with a common key and transmitted from a server;
  - a second step of decrypting by the system the received common key-encrypted program to generate a raw program; and
  - a third step of re-encrypting by the system the raw program with the inherent key and storing the re-encrypted program in the external memory as a new inherent key-encrypted program.
- 15 2. The program update method of claim 1, further comprising the steps of:
  - receiving by the system common key information transmitted from the server; and
  - generating by the system a raw common key using the received common key information,

20 wherein at the second step, the raw common key is used to decrypt the common key-encrypted program.

- 3. The program update method of claim 2, wherein the common key information includes an encrypted common key generated by encrypting the raw common key with a raw first intermediate key, and an encrypted first intermediate key generated by encrypting the raw

first intermediate key with a raw second intermediate key.

4. The program update method of claim 1, wherein:

the LSI device includes an internal memory in which inherent key

5 information is stored;

the system uses the inherent key information stored in the internal memory

to generate a raw inherent key at boot-up of the system; and

at the third step, the raw inherent key is used for re-encrypting the raw  
program.

10

5. The program update method of claim 4, wherein the inherent key information includes  
an encrypted inherent key generated by encrypting the raw inherent key with a raw third  
intermediate key and an encrypted second intermediate key generated by encrypting the  
raw third intermediate key with a raw fourth intermediate key.

15

6. The program update method of claim 4, wherein the generated raw inherent key is  
stored in a register of the LSI device and is used for decrypting the inherent key-encrypted  
program to a raw program for execution of the inherent key-encrypted program.

20 7. The program update method of claim 1, wherein:

the LSI device includes a boot ROM in which a boot program is stored;

the external memory includes an acquisition program for establishing data  
transmission between the LSI device and a server; and

the system executes reception of the common key-encrypted program based

25 on the acquisition program stored in the external memory, and controls update processing

performed after the reception of the common key-encrypted program based on the boot program stored in the boot ROM.

8. The program update method of claim 1, further comprising the step of receiving a  
5 HASH value of the raw program transmitted from the server,

wherein at the second step, the received HASH value is used to perform a  
HASH verification on the decrypted raw program.

9. A server which operates for program update in a system including an LSI device, the  
10 server executing:

a first step of receiving from the system an ID of the LSI device and an  
application ID which is identification information of an update object program;

a second step of referring a first table which indicates correspondences  
between application IDs and LSI IDs to determine whether or not the update object  
15 program is transmitted to the system; and

if it is determined at the second step that the update object program is  
transmitted to the system, a third step of transmitting to the system a common key-  
encrypted program generated by encrypting the update object program with a common key  
and common key information from which the common key is derived.

20

10. The server of claim 9, executing:

a fourth step of receiving from the system a signal which requests  
application inherent information necessary for execution of the update object program; and

a fifth step of referring to a second table which indicates correspondence  
25 between a transmission history of the application inherent information and the LSI IDs to

determine whether or not the application inherent information requested at the fourth step is transmitted.

11. The server of claim 9, wherein the common key information includes an encrypted

5 common key generated by encrypting a raw common key with a raw first intermediate key and an encrypted first intermediate key generated by encrypting the raw first intermediate key with a raw second intermediate key.